mHz!

En este nuestro número # 1 encontrarás ...

En la red podrás vernos en mHz.8m.com

EDITORIAL

Bueno les cuento desde donde surge la MHZ (METAL HACK ZINE). Metalhack es una lista que hace ya un año que cree. Hace un tiempo tuve la idea de sacar una E-Zine y me puse en contacto con una de las personas que mas hace crecer la lista, ella es Marixta. Juntos Formamos el MHT (METAL HACK TEAM).
Hoy metalhack tiene 200 suscriptos y esperamos que ese numero crezca.
Nuestra ideología, es la de compartir la info que tenemos y crecer de esa manera. Nuestra E-Zine es gratuita y lleva mucho tiempo y dedicación por parte de nosotros los miembros del MHT, así que todas las contribuciones que puedas hacer van a ser muy fructíferas para nuestra E-Zine.
Elegimos este Formato dado que el txt es demasiado aburrido y no permite la inclusión de colores y fotografías. Si bien el txt es un formato muy utilizado y que ocupa poco espacio, es muy aburrido. Esta E-Zine si bien es de Hack posee algunas variantes y puede tener sus artículos de opinión, pero principalmente se basa en el Hacking.
Nosotros no nos hacemos cargo de la mala utilización que hagas de esta info. La idea es que sepas un poco más, mas que nada se tiene que tomar el Hacking como un desafío, no como un fin para destruir u obtener dinero.
Si reproducís algunos de los artículos que están en mHz, por favor, cita el autor con su respectivo mail.
Te recuerdo que si querés estar informado de lo que sucede en el Hack te suscribas a la MHL (MetalHackList) enviando un mail en blanco a metalhack-subscribe@yahoogroups.com
Y si querés unirte al MHT envíame un mail a ripper@interlap.com.ar detallando en que área te desenvolvés.
Bueno esto es todo, espero que les guste la mHz, con el tiempo se va a ir volviendo mas técnica, así que no dejen de visitar la page, para bajarse los últimos números, ya veremos la forma de implementar el envío por mail.

Ripper

STAFF

Los miembros del Staff del MHT son:

Ripper (ripper@interlap.com.ar) Seccion : hacking

Marixta: (marixta1998@hotpop.com) sección : telefonía

Se agradece a Crazywoman y a Kermit por colaborar en este número.

TELNET por Ripper

(ripper@interlap.com.ar)

Antes de leer este articulo es recomendable que tengas en cuenta el concepto de puertos. Es un texto resumido de lo que es telnet, mas que nada para que te des una idea, hay textos más técnicos en la Red.

TEORIA

1) ¿Qué es Telnet?
Para decirlo de una manera sencilla telnet es aquel protocolo (te doy un Ej.: el Tcp/ Ip) que te permite establecer una conexión con otro ordenador. Telnet es usado por http y los Ftp para que te des una idea.

2) Ok, pero ¿para que quiero usar telnet?
Fácil para el control de datos. Algunas que otras utilidades, tontas, pero en fin, por Ej.: mandar mails anónimos, leer tus mails, borrarlos, etc.

3) No se nada de Linux, puede hacer telnet desde Windows?
La respuesta es Si, La mayoría de los SO (sistemas operativos) tienen este comando.

PRACTICA

Un pequeño Ej. de como hacer telnet:

* hacer Telnet a otra maquina telnet ripper.pc.ar XX (acá pones el puerto)

Vas a visualizar lo siguiente

Telnet ripper.pc.ar XX
Trying 132.130.25.52 PORT XX
Connected to ripper.pc.ar

Supuestamente estas conectado, pero para establecer una buena comunicación tenés que tener en cuenta varias cosas:

* El login y el pass, antes con usar guest alcanzaba, ahora es un poco mas complejo
Una vez que pusiste el login y el pass adecuado, tenés que elegir el tipo de modulación (VT 100 ANSI, etc) Te conviene poner VT 100 que es la mas común, es probable que se configure automáticamente, depende del cliente.
* Telnet es un entorno de comandos, (Ej. DOS) es decir, no tenés una interfaz grafica para moverte dentro del sistema, así que tenés que saber lo siguientes comandos:
OPEN este comando te permite abrir una conexión remota
CLOSE Cierra la conexión Telnet
QUIT Salís de telnet

SET ECHO este comando es muy importante ya que si tenés problemas con la visualización de lo que estas escribiendo esto te lo resuelve, es probable que veas la pantalla en blanco, esto arregla eso.

FIN

PUERTOS por Ripper

(ripper@interlap.com.ar)

Puertos más comunes:

9	discard	Basura
11	systat	Te da la data de los usuarios
13		Fecha y hora
15	netstat	
17/tcp	qotd	Quote of the Day
19	chargen	Generador de caracteres
21	ftp	transf
22/tcp	ssh	SSH Remote Login Protocol
23	telnet	Login pass
25	smpt	smtp
37	time	hora
38/tcp	rap	RouteAccessProtocol
39	rlp	Localización del recurso
42/tcp	name server	Hostname Server
43	whois	Información sobre la red objetivo
49/tcp	tacacs	LoginHostProtocol(TACACS)
50/tcp	re-mail-ck	RemoteMailCheckingProtocol
53	domain	Nombre de la maquina
63/tcp	whois++	
69/tcp	tftp	TrivialFileTransfer
70	gopher	
79	finger	info. de los users
80	http	ServidorWeb
88/tcp	kerberos	Kerberos
107	rtelnet	Telnet remoto
109/tcp	pop2	PostOfficeProtocol-Version2
110	pop3	pop3 (e mail)
111/tcp	sunrpc	SUN Remote Procedure Call
113/tcp	auth	Authentication Service
115/tcp	sftp	Simple File Transfer Protocol
117/tcp	uucp-path	UUCP Path Service
119	nntp	Grupos de noticias Usenet
133/tcp	statsrv	Statistics Service
136/tcp	profile	PROFILE Naming System
137/tcp	netbios-ns	NETBIOSNameService
137/udp	netbios-ns	NETBIOSNameService
138/tcp	netbios-dgm	NETBIOSDatagramService
138/udp	netbios-dgm	NETBIOSDatagramService
139/tcp	netbios-ssn	NETBIOSSessionService
139/udp	netbios-ssn	NETBIOSSessionService
143/tcp	imap	InternetMessageAccessProtocol
144/tcp	news	News
161/tcp	snmp	SNMP
194/tcp	irc	InternetRelayChatProtocol
213/tcp	ipx	IPX

220/tcp	imap3	InteractiveMailAccessProtocolv3
443	shttp	server by web
512/	udp biff	notifiacion de mail
513/tcp	rlogin	remote login
513/udp	who	quien? (te dice quien esta)
514/tcp	shell	Shell remota
514/udp	syslog	
515/tcp	printer	spooler
520	route	Protocolo de información routing
529/tcp	irc-serv	IRC-SERV

Puertos que abren los Troyanos

Puerto 21 - Blade Runner, Dolly Trojan, Fore, Invisible FTP, WebEx, WinCrash
puerto 23 - Tiny Telnet Server
puerto 25 - Antigen, Email Password Sender, Haebu Coceda, Shtrilitz Stealth, Terminator, WinPC, WinSpy
puerto 31 - Hackers Paradise
puerto 80 - Executor
puerto 456 - Hackers Paradise
puerto 555 - Ini-Killer, Phase Zero, Stealth Spy
puerto 666 - Satanz Backdoor
puerto 1001 - Silencer, WebEx
puerto 1011 - Doly Trojan
puerto 1170 - Psyber Stream Server, Voice
puerto 1234 - Ultors Trojan
puerto 1245 - VooDoo Doll
puerto 1492 - FTP99CMP
puerto 1600 - Shivka-Burka
puerto 1807 - SpySender
puerto 1981 - Shockrave
puerto 1999 - BackDoor
puerto 2001 - Trojan Cow
puerto 2023 - Ripper
puerto 2115 - Bugs
puerto 2140 - Deep Throat, The Invasor
puerto 2801 - Phineas Phucker
puerto 3024 - WinCrash
puerto 3129 - Masters Paradise
puerto 3150 - Deep Throat, The Invasor
puerto 3700 - Portal of Doom
puerto 4092 - WinCrash
puerto 4590 - ICQTrojan
puerto 5000 - Sockets de Troie
puerto 5001 - Sockets de Troie
puerto 5321 - Firehotcker
puerto 5400 - Blade Runner
puerto 5401 - Blade Runner
puerto 5402 - Blade Runner
puerto 5569 - Robo-Hack

puerto 5742 - WinCrash
puerto 6670 - DeepThroat
puerto 6771 - DeepThroat
puerto 6969 - GateCrasher, Priority
puerto 7000 - Remote Grab
puerto 7300 - NetMonitor
puerto 7301 - NetMonitor
puerto 7306 - NetMonitor
puerto 7307 - NetMonitor
puerto 7308 - NetMonitor
puerto 7789 - ICKiller
puerto 9872 - Portal of Doom
puerto 9873 - Portal of Doom
puerto 9874 - Portal of Doom
puerto 9875 - Portal of Doom
puerto 9989 - iNi-Killer
puerto 10067 - Portal of Doom
puerto 10167 - Portal of Doom
puerto 11000 - Senna Spy
puerto 11223 - Progenic trojan
puerto 12223 - Hack´99 KeyLogger
puerto 12345 - GabanBus, NetBus
puerto 12346 - GabanBus, NetBus
puerto 12361 - Whack-a-mole
puerto 12362 - Whack-a-mole
puerto 16969 - Priority
puerto 20001 - Millennium
puerto 20034 - NetBus 2 Pro
puerto 21544 - GirlFriend
puerto 22222 - Prosiak
puerto 23456 - Evil FTP, Ugly FTP
puerto 26274 - Delta
puerto 30100 al 02 - NetSphere
puerto 31337 - Back Orifice
puerto 31338 - Back Orifice, DeepBO
puerto 31339 - NetSpy DK
puerto 31666 - BOWhack
puerto 33333 - Prosiak
puerto 34324 - BigGluck, TN
puerto 40412 - The Spy
puerto 40421al 26 - Masters Paradise
puerto 47262 - Delta
puerto 50505 - Sockets de Troie
puerto 50766 - Fore
puerto 53001 - Remote Windows Shutdown
puerto 54320 - Back Orifice 2000
puerto 54321 - Back Orifice 2000
puerto 61466 - Telecommando
puerto 65000 – Devil
fuentes consultadas www.ezkracho.com.ar

Virus, por Crazywoman

(doppelgang@concordia.com.ar)

Virus Informáticos

Un virus es simplemente un programa. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco. De todas formas, dentro del término "virus informático" se suelen englobar varios tipos de programas.

A continuación haremos un pequeño repaso a cada uno de ellos poniendo de manifiesto sus diferencias. La clasificación más usual es la siguiente:

Virus "puro"

Caballo de Troya

Bomba Lógica

Gusano o Worm

Todos estos programas tienen en común la creación de efectos perniciosos; sin embargo, no todos pueden ser considerados como virus propiamente dichos.

Virus "Puro"

Un verdadero virus tiene como características más importantes la capacidad de copiarse a sí mismo en soportes diferentes al que se encontraba originalmente, y por supuesto hacerlo con el mayor sigilo posible y de forma transparente al usuario; a este proceso de auto réplica se le conoce como "infección", de ahí que en todo este tema se utilice la terminología propia de la medicina: "vacuna", "tiempo de incubación", etc. Como soporte entendemos el lugar donde el virus se oculta, ya sea fichero, sector de arranque, partición, etc.
Un virus "puro" también debe modificar el código original del programa o soporte objeto de la infección, para poder activarse durante la ejecución de dicho código; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar así de forma trasparente al usuario.

Caballo de Troya

Al contrario que el virus puro, un Caballo de Troya es un programa maligno que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este ultimo. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

Bomba Lógica

Se trata simplemente de un programa maligno que permanece oculto en memoria y que solo se activa cuando se produce una acción concreta, predeterminada por su creador: cuando se llega a una fecha en concreto (Viernes 13), cuando se ejecuta cierto programa o cierta combinación de teclas, etc.

Gusano o Worm

Por último, un gusano es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la RAM, siendo ésta su única acción maligna.
La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno o de varios de estos programas: por ejemplo, los virus como el Viernes 13 son capaces de infectar otros archivos, siendo así virus puro, pero también realizan su efecto destructivo cuando se da una condición concreta, la fecha Viernes 13, característica propia de una bomba lógica; por último, se oculta en programas ejecutables teniendo así una cualidad de Caballo de Troya. De ahí la gran confusión existente a este respecto.

Formas De Infección

Antes de nada, hay que recordar que un virus no puede ejecutarse por si solo, necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse a un programa portador necesita modificar la estructura de este, para que durante su ejecución pueda realizar una llamada al código del virus.

Las partes del sistema más susceptibles de ser infectadas son el sector de arranque de los disquetes, la tabla de partición y el sector de arranque del disco duro, y los ficheros ejecutables (*.EXE y *.COM). Para cada una de estas partes tenemos un tipo de virus, aunque muchos son capaces de infectar por sí solos estos tres componentes del sistema.

En los disquetes, el sector de arranque es una zona situada al principio del disco, que contiene datos relativos a la estructura del mismo y un pequeño programa, que se ejecuta cada vez que arrancamos desde disquete.

En este caso, al arrancar con un disco contaminado, el virus se queda residente en memoria RAM, y a partir de ahí, infectara el sector de arranque de todos los disquetes a los que se accedan, ya sea al formatear o al hacer un DIR en el disco, dependiendo de cómo esté programado el virus.

El proceso de infección consiste en sustituir el código de arranque original del disco por una versión propia del virus, guardando el original en otra parte del disco; a menudo el virus marca los sectores donde guarda el boot original como en mal estado, protegiéndolos así de posibles accesos, esto suele hacerse por dos motivos: primero, muchos virus no crean una rutina propia de arranque, por lo que una vez residentes en memoria, efectúan una llamada al código de arranque original, para iniciar el sistema y

así aparentar que se ha iniciado el sistema como siempre, con normalidad. Segundo, este procedimiento puede ser usado como técnica de ocultamiento.

Normalmente un virus completo no cabe en los 512 bytes que ocupa el sector de arranque, por lo que en éste suele copiar una pequeña parte de si mismo, y el resto lo guarda en otros sectores del disco, normalmente los últimos, marcándolos como defectuosos. Sin embargo, puede ocurrir que alguno de los virus no marquen estas zonas, por lo que al llenar el disco estos sectores pueden ser sobrescritos y así dejar de funcionar el virus.

La tabla de partición esta situada en el primer sector del disco duro, y contiene una serie de bytes de información de cómo se divide el disco y un pequeño programa de arranque del sistema. Al igual que ocurre con el boot de los disquetes, un virus de partición suplanta el código de arranque original por el suyo propio; así, al arrancar desde disco duro, el virus se instala en memoria para efectuar sus acciones. También en este caso el virus guarda la tabla de partición original en otra parte del disco, aunque algunos la marcan como defectuosa y otros no. Muchos virus guardan la tabla de partición y a ellos mismos en los últimos sectores de disco, y para proteger esta zona, modifican el contenido de la tabla para reducir el tamaño lógico del disco. De esta forma el DOS no tiene acceso a estos datos, puesto que ni siquiera sabe que esta zona existe.

Casi todos loa virus que afectan la partición también son capaces de hacerlo en el boot de los disquetes y en los ficheros ejecutables; un virus que actuara sobre particiones de disco duro tendría un campo de trabajo limitado, por lo que suelen combinar sus habilidades.

Con todo, el tipo de virus que más abunda es el de fichero; en este caso usan como vehículo de expansión los archivos de programa o ejecutables, sobre todo .EXE y . COM, aunque también a veces .OVL, BIN y .OVR. AL ejecutarse un programa infectado, el virus se instala residente en memoria, y a partir de ahí permanece al acecho; al ejecutar otros programas, comprueba si ya se encuentran infectados. Si no es así, se adhiere al archivo ejecutable, añadiendo su código al principio y al final de éste, y modificando su estructura de forma que al ejecutarse dicho programa primero llame al código del virus devolviendo después el control al programa portador y permitiendo su ejecución normal.

Este efecto de adherirse al fichero original se conoce vulgarmente como "engordar" el archivo, ya que éste aumenta de tamaño al tener que albergar en su interior al virus, siendo esta circunstancia muy útil para su detección. De ahí que la inmensa mayoría de los virus sean programados en lenguaje ensamblador, por ser el que genera el código más compacto, veloz y de menor consumo de memoria; un virus no seria efectivo si fuera fácilmente detectable por su excesiva ocupación en memoria, su lentitud de trabajo o por un aumento exagerado en el tamaño de los archivos infectados. No todos los virus de fichero quedan residentes en memoria, si no que al ejecutarse se portador, éstos infectan a otro archivo, elegido de forma aleatoria de ese directorio o de otros.

Efectos destructivos de los virus

Los efectos perniciosos que causan los virus son variados; entre éstos se encuentran el formateo completo del disco duro, eliminación de la tabla de partición, eliminación de archivos, ralentización del sistema hasta limites exagerados, enlaces de archivos destruidos, archivos de datos y de programas corruptos, mensajes o efectos extraños en la pantalla, emisión de música o sonidos.

Formas de ocultamiento

Un virus puede considerarse efectivo si, además de extenderse lo más ampliamente posible, es capaz de permanecer oculto al usuario el mayor tiempo posible; para ello se han desarrollado varias técnicas de ocultamiento o sigilo. Para que estas técnicas sean efectivas, el virus debe estar residente en memoria, puesto que debe monitorizar el funcionamiento del sistema operativo. La base principal del funcionamiento de los virus y de las técnicas de ocultamiento, además de la condición de programas residentes, la intercepción de interrupciones. El DOS y los programas de aplicación se comunican entre sí mediante el servicio de interrupciones, que son como subrutinas del sistema operativo que proporcionan una gran variedad de funciones a los programas. Las interrupciones se utilizan, por ejemplo, para leer o escribir sectores en el disco, abrir ficheros, fijar la hora del sistema, etc. Y es aquí donde el virus entra en acción, ya que puede sustituir alguna interrupción del DOS por una suya propia y así, cuando un programa solicite un servicio de esa interrupción, recibirá el resultado que el virus determine.

Entre las técnicas más usuales cabe destacar el ocultamiento o stealth, que esconde los posibles signos de infección del sistema. Los síntomas más claros del ataque de un virus los encontramos en el cambio de tamaño de los ficheros, de la fecha en que se crearon y de sus atributos, y en la disminución de la memoria disponible.

Estos problemas son indicadores de la posible presencia de un virus, pero mediante la técnica stealth es muy fácil (siempre que se encuentre residente el virus) devolver al sistema la información solicitada como si realmente los ficheros no estuvieran infectados. Por este motivo es fundamental que cuando vayamos a realizar un chequeo del disco duro arranquemos el ordenador con un disco de sistema totalmente limpio.

La auto encriptación o self-encryption es una de las técnicas víricas más extendidas. En la actualidad casi todos los nuevos ingenios destructivos son capaces de encriptarse cada vez que infectan un fichero, ocultando de esta forma cualquier posible indicio que pueda facilitar su búsqueda. No obstante, todo virus encriptado posee una rutina de desencriptación, rutina que es aprovechada por los antivirus para ubicar el origen de la infección.

El mayor avance en técnicas de encriptación viene dado por el polimorfismo. Gracias a él un virus no sólo es capaz de encriptarse sino que además varía la rutina empleada cada vez que infecta un fichero. De esta forma resulta imposible encontrar coincidencias entre distintos ejemplares del mismo virus y ante esta técnica el tradicional método de búsqueda de cadenas características se muestra inútil.

Otra técnica básica de ocultamiento es la intercepción de mensajes de error del sistema. Supongamos que un virus va a infectar un archivo de un disco protegido contra escritura; al intentar escribir en el obtendríamos el mensaje: "Error de protección contra escritura leyendo unidad A Anular, Reintentar, Fallo?", por lo que descubriríamos el anormal funcionamiento de nuestro equipo. Por eso, al virus le basta con redireccionar la interrupción a una rutina propia que evita la salida de estos mensajes, consiguiendo así pasar desapercibido.

Prevención, detección y eliminación

Es recomendable seguir estas pautas para mantenerse alejado de una posible infección:

1) Usar regularmente un programa anti-virus. Y por supuesto, de nada vale usar algún antivirus si no lo mantenemos actualizado con los upgrades, updates o add-ons correspondientes. Actualmente, las actualizaciones son diarias o al menos semanales. No existen los "virus demasiados nuevos y sin antídotos", la reacción de las casas de antivirus es inmediata en todos los casos. Pero mejor cabe preguntarse si la nuestra también lo es a la
hora de actualizarse.

2) No abrir ningún mensaje ni archivo recibido a través del correo electrónico de fuentes desconocidas o muy poco conocidas. En el caso de personas conocidas, se deben igualmente tomar las precauciones correspondientes. Asegurarse con esa persona del envío ("Melissa" y otros pueden ser enviados por conocidos que ignoran estar mandando el virus en sus mensajes), y nunca ejecutarlos, sino guardarlos en una carpeta temporal y pasarle a esa carpeta dos o tres antivirus actualizados antes de tomar la opción de ejecutarlos (.EXE) o abrirlos (.DOC, .RTF, etc.). Pero ante cualquier duda, simplemente se debe optar por borrar el mensaje (y archivos adjuntos).

3) Estar informado de cómo operan los virus, y de las novedades sobre estos, alertas y anuncios críticos.

4) No bajar nada de sitios Web de los que no tenga referencias de seriedad, o que no sean medianamente conocidos. Y si se bajan archivos, proceder como los archivos adjuntos. Copiarlos a una carpeta y revisarlos con dos o tres antivirus actualizados antes de optar por ejecutarlos o abrirlos.

Virus de macros

Esta entre las novedades surgidas últimamente en el mundo de los virus, aunque no son totalmente nuevos, parece que han esperado hasta 1995 para convertirse en una peligrosa realidad. Por desgracia, ya existe un número importante de virus de este tipo catalogados, que han sido escritos en WordBasic, el potente lenguaje incluido en Microsoft Word.

Estos virus sólo afectan a los usuarios de Word para Windows y consisten en un conjunto de macros de este procesador de textos. Aunque el peligro del virus se restringe a los usuarios de Word, tiene una importante propagación ya que puede infectar cualquier texto, independientemente de la plataforma bajo la que éste se ejecute: Mac, Windows 3.x, Windows NT, W95, W98 y OS/2. Este es el motivo de su

peligrosidad, ya que el intercambio de documentos en disquete o por red es mucho más común que el de ejecutables.

El primer virus de este tipo que salió a la luz se llamaba "WordMacro/DMV" y era inofensivo, ya que sólo anunciaba su presencia y guardaba un informe de sus acciones. Escrito por Joel McNamara para el estudio de los virus de macros, fue desarrollado en 1994 pero su autor guardó el resultado hasta que observó la aparición del virus conocido por "WordMacro/Concept". Tras ello, McNamara decidió hacer público su desarrollo esperando que la experiencia adquirida sirviera de enseñanza para todos los usuarios. Y aunque probablemente tenga un efecto negativo, McNamara ha publicado también las pautas para crear virus que afecten a los ficheros de Excel.

Software Antivirus

Para combatir la avalancha de virus informáticos se creó el software antivirus. Estos programas suelen incorporar mecanismos para prevenir, detectar y eliminar virus. Para la prevención se suelen usar programas residentes que alertan al usuario en todo momento de cualquier acceso no autorizado o sospechoso a memoria o a disco, por lo que resultan sumamente útiles al impedir la entrada del virus y hacerlo en el momento en que este intenta la infección, facilitándonos enormemente la localización del programa maligno. Sin embargo presentan ciertas desventajas, ya que al ser residentes consumen memoria RAM, y pueden también resultar incompatibles con algunas aplicaciones. Por otro lado, pueden llegar a resultar bastante molestos, puesto que por lo general suelen interrumpir nuestro trabajo habitual con el ordenador avisándonos de intentos de acceso a memoria o a disco que en muchos casos provienen de programas legítimos. A pesar de todo, son una medida de protección excelente y a ningún usuario debería faltarle un programa de este tipo.

A la hora de localizar virus, los programas usados son los detectores o scanners. Normalmente estos programas chequean primero la memoria RAM, después las zonas criticas del disco como el boot o partición, y por ultimo los ficheros almacenados en él.

Los productos antivirus han mejorado considerablemente sus algoritmos de búsqueda, aunque en la actualidad la exploración de cadenas sigue siendo la técnica más empleada. Pero el aumento imparable del número de virus y las técnicas de camuflaje y auto modificación que suelen emplear hacen que la búsqueda a través de una cadena genérica sea una tarea cada vez más difícil. Por ello, es cada día es más frecuente el lanzamiento de antivirus con técnicas heurísticas.

La detección heurística es una de las fórmulas más avanzadas de remoción de virus. La búsqueda de virus mediante esta técnica se basa en el desensamblado del código del programa que se intenta analizar con el objetivo de encontrar instrucciones (o un conjunto de ellas) sospechosas. Sin duda, lo mejor es disponer de un antivirus que combine la búsqueda de cadenas características y además cuente con técnicas heurísticas.

Gracias a la heurística se buscan programas que puedan quedarse residentes o que sean capaces de capturar aplicaciones que se estén ejecutando, código preparado para mover o sobrescribir un programa en memoria, código capaz de auto modificar ejecutables, rutinas de encriptación y desencriptación, y otras actividades propias de los virus.

Cómo Reaccionar Ante Una Infección

La prevención y la compra de un buen antivirus son las mejores armas con las que cuenta el usuario ante el ataque de los virus. Sin embargo, siempre cabe la posibilidad de que en un descuido se introduzca un inquilino no deseado en nuestra PC. Ante esta situación lo primero que debemos hacer es arrancar la PC con un disco de sistema totalmente libre de virus. Posteriormente deberemos pasar un antivirus lo más actualizado posible, ya que si es antiguo corremos el riesgo de que no detecte mutaciones recientes o nuevos virus.

Bibliografía consultada

ALDEGANI, Gustavo. VIRUS INFORMATICO. Normas de Seguridad. 1994, KRON Editorial.

PCUSERS Extra No. 29. Febrero de 2000.

video SOFT (Maldonado, Uruguay) - http://www.videosoft.net.uy. VSantivirus No. 164 - Año 4 - Martes 19 de diciembre de 2000.

http://www.mflor.mx/materias/temas/virus/virus.htm.

Los Sistemas Operativos

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

por Kermit <buanzo@uol.com.ar>

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Que tal gente! Espero que esta no sea mi primer y ultimo saludo, sino que deseo que este sea el primero de muchos en esta nueva e-Zine que estamos intentando hacer entre la gente que formamos el equipo de redacción de la “mHz”.

Como se darán cuenta por el titulo de este articulo, voy a empezar a tratar este apasionante tema de los Sistemas Operativos, ese conjunto que mezcla las palabras 'kernel', 'administración procesos' (y memoria, y dispositivos, y usuarios), 'seguridad', 'sistema de archivos' y tantas otras que me estoy olvidando, o que inconscientemente no me parecerán tan importantes, en un solo concepto único, que es, justamente EL SISTEMA OPERATIVO. (de ahora en mas, "OS" por Operating System).

Bien, pienso organizar esta serie de artículos logrando primero un acercamiento general a lo que ES un OS, conceptual y prácticamente, tipos de OS's (monousuario, multiusuario, de kernel monolítico, etc), y diferentes OS's (DOS, Windows (bue... DOS) y sus diferentes versiones / variantes, Unix, Linux) y las diferencias que radican entre ellos tanto a nivel operativo como a nivel seguridad / funcionalidad, etc.

Quiero que por favor sus dudas, criticas (constructivas, por favor), consejos, ideas, etc, me los hagan llegar a buanzo@uol.com.ar - Si es algo que concierne a la revista y no específicamente a mi articulo, sírvanse escribir a la casilla de la E-Zine.

OK, basta de cháchara, y comencemos a hablar de....

- Capitulo 1 -

INTRODUCCION A LOS SISTEMAS OPERATIVOS

-=-

* QUE es un Sistema Operativo?

Bueno, todos ustedes saben para que sirve el teclado, el mouse, el monitor, la disquetera, la lectora de CD-ROM, DVD, el disco rígido, la RAM... bueno, todos estos RECURSOS (resources) y / o DISPOSITIVOS (devices) son controlados, administrados, manejados por el OS. O sea, el OS se encarga de administrar el uso de estos recursos y, dependiendo del tipo de sistema operativo, repartir el uso de estos dispositivos y recursos entre los diferentes programas / procesos que se estén ejecutando. En caso de un sistema monotarea (el viejo MS-DOS por ejemplo) los procesos generalmente obtienen el control absoluto de los recursos. Es por eso que hay que tener cuidado al ejecutar programas MS-DOS desde Windows 9x/2000/etc..... por problemas de implementación de las maquinas virtuales DOS se puede llegar a colgar todo el sistema. Lindo, no? Se explicara que es una maquina virtual mas adelante, por el momento imaginen que es una caja boba que simula ser otra PC, pero que en verdad no lo es. Es solo una simulación de otra PC dentro de tu PC.

Muchas veces el shell (interfaz, pero literalmente concha, cáscara) es tomado como sistema operativo. Por ejemplo, en el viejo MS-DOS, el COMMAND.COM (digamos, el C:\> _) NO ES el sistema operativo! Es solamente el interprete entre el usuario Y el sistema operativo. El COMMAND.COM no se encarga de administrar la memoria, ni el acceso a disco ni nada de esto! Esto lo hacen el MSDOS.SYS y el IO.SYS, que son cargados gracias a que la MBR (master boot record, registro maestro de boot [boot=inicio]) contiene un programa que indica como cargarlos en memoria y ejecutarlos.

Otro ejemplo peor: Windows... no es un sistema operativo, es un entorno operativo, un shell muy ampliado. La mayoría de las funciones básicas de administración de los recursos siguen siendo como en DOS!

Esto es lo que crea problemas, colgaduras, incompatibilidades, etc.

En teoría Microsoft esta corrigiendo sus errores, y en Windows ME se supone que ya es totalmente 32 bits, y no solo un programa visual ultra fashion shell ejecutándose encima del viejo DOS... Podrán? :)

Que otras alternativas existen, entonces, al Windows, pero que de por si funcionen bien? El Linux, el FreeBSD, etc. Para mas información, puede ir a www.linux.org, o si son de Argentina visiten el LUGAr (Linux Users' Group Argentina) en www.linux.org.ar.

Entonces, que es un Sistema Operativo? Es básicamente un Kernel (núcleo) que brinda las funciones básicas del sistema, sumado a un conjunto de utilidades, programas, de productividad y administración. Y quizá algún jueguito :)

* Tipos de Sistemas Operativos

Podemos clasificar a los sistemas operativos bajo un sistema doble:

Tarea ----- Monotarea

|--- Multitarea

Usuarios ----- Monousuario

|--- Multiusuario

La diferencia entre los términos Monotarea y Multitarea radica en la capacidad del sistema operativo para ejecutar varios programas concurrentemente, o sea, al mismo tiempo. Si un OS es multitarea no necesariamente tiene que ser multiusuario. No confundir con el hecho de que por ejemplo tengamos un servidor FTP en Windows 98 que nos permita ingresar con diferentes usuarios! No se esta iniciando una sesión del sistema para cada uno de esos usuarios, simplemente es un programita que te da o no acceso al sistema de archivos del FTP, con ciertos permisos, nada mas.

Entonces, un sistema multiusuario (como Unix o Windows NT) por que son multiusuario? Porque la diferencia entre usuario y usuario EXISTE, no solo a nivel personalización (el escritorio de Windows y la configuración del Outlook, por ejemplo), sino a nivel SISTEMA. Diferentes niveles de privilegios, una sesión no interfiere con la otra, etc, etc. Y porque cuando el OS te pide usuario y clave (independientemente del m,todo de conexión que utilices, ya veremos esto en próximas entregas) se inicializa un entorno (conjunto de variables, privilegios, etc en el que la sesión del usuario existe) único para ese usuario.

Bien, con esto doy por terminada la introducción básica a los sistemas operativos. Esto fue un vistazo MUY general y por arriba de lo que verdaderamente un hacker debe saber sobre sistemas operativos, también debo hablar sobre librerías compartidas, acceso a la memoria, manejo de procesos o sea, todas las operaciones de bajo nivel que realiza el kernel (núcleo del sistema).

Cualquier duda, pregunta, comentario, critica constructiva o idea temática sobre este articulo, háganmela llegar a buanzox@usa.net

Chau!

Sistema de Telefonía Celular por (...)

Maritxa1998@hotpop.com

ESTACIÓN BASE Y CELDA

La estación base (EB) es el punto a través del cual se comunican los móviles con el sistema. Su función consiste en recibir las señales radiales desde los móviles y enviar las señales hacia los mismos. Cada estación base está compuesta por: equipamiento de transmisión y recepción, torre, antenas, fuente de alimentación eléctrica, baterías y alarmas. Cada estación base genera un área de cobertura (área geográfica a la que, en función de una determinada potencia aplicada, una antena puede cubrir con suficiente intensidad de señal), que es donde existe la mayor probabilidad de entablar contacto radial con un móvil. La potencia y altura de la antena se regula para dimensionar el área de cobertura, determinándose su tamaño por la densidad del tráfico previsto, topografía, área rural o urbana, etc.. Una estación base puede estar conectada al sistema por medio de cableado fijo o por medio de microondas. Su comunicación con los móviles es por radiofrecuencia, con canales simultáneos de comunicación full duplex. La transmisión desde la estación base hacia los móviles se denomina FORWARD LINK o DQWNLINK y la transmisión desde los móviles hacia la estación base se denomina REVERSE LINK o UPLINK. Cada estación base dedica, además, un receptor de localización para: a) monitorear los “reverse voice channels (canales de voz de retorno desde el móvil a la estación base) de dentro y cerca de la celda y b) reportar la información de intensidad de señal recibida al sistema (RSSI). Cuando se alcanza el nivel de señal definido como para efectuar la entrega del manejo de la llamada a otra estación base (handoff”), el sistema supervisa la realización del mismo.

El área de cobertura generada por una Estación Base se denomina celda. El termino celda en inglés se expresa “cell”. Un sistema constituido por “cells” se denomina con el término inglés “cellular”, de allí surge que en castellano se conozca a este sistema como telefonía celular. Si bien no responde a una forma geométrica precisa, se conceptualiza a una celda como un hexágono, dado que esta forma se asemeja a la circular pero tiene seis lados iguales que son apareables para conformar conjuntos de celdas sin espacios en blanco ni superposiciones, denominados “clusters’. Esta estructura es la óptima para permitir el re-uso de la misma frecuencia en celdas no adyacentes. La cantidad de estaciones base (celdas) necesarias para dar cobertura a una región es muy variable. La red de Telefónica Comunicaciones Personales tiene actualmente más de 540 celdas o sitios celulares, servidas en su mayoría por una estación base, y las restantes por extensores de celda o repetidores.

Existen diferentes tipos de terminales para los usuarios de telefonía móvil (celular), con distintas características y potencia. Los terminales personales (también llamados portables o portátiles) son equipos de comunicaciones celulares de tamaño y peso reducido, típicamente para uso personal y especialmente adaptados al ámbito urbano, donde las celdas son de menor tamaño relativo y la intensidad de señal es mayor. Son los equipos de menor potencia (0,6 W), cuyas continuas mejoras en el diseño les agregan cada vez más prestaciones sin aumentar su tamaño ni su peso.

Los terminales transportables (Carry) son equipos de tamaño mediano (tipo pequeña valija), con batería propia y mayor alcance, con una potencia de 3 W. Por su tamaño pueden ser transportados manualmente y también conectados a la batería de un vehículo o a la red eléctrica domiciliaria para recargarlos o para reemplazar la batería. Están especialmente adaptados al uso en áreas de relativamente baja intensidad de señal (rurales o suburbanas).

Los terminales móviles son los equipos especialmente diseñados para instalarse en un vehículo. Son los de mayor capacidad de recepción y emisión (3 W). Como no disponen de batería propia, utilizan la del vehículo. Especialmente adaptados para el uso en rutas y áreas rurales, donde el tamaño de las celdas es mayor y, por ello, hay zonas de menor intensidad de señal.

COBERTURA

La distancia existente entre la antena y el terminal determina la intensidad de señal disponible: a mayor distancia de la antena, menor intensidad de señal. Es decir que cuanto más cerca se encuentre el móvil del límite de la celda, mayor será la potencia requerida para poder comunicarse.

Si un terminal de 0,6 W (personal) se encuentra cercano a la estación base, podrá captar la señal aun estando dentro de un edificio; a dicha distancia de la antena se considera que la cobertura es “indoor” (puertas adentro).

Si este mismo terminal se alejara un poco más de la estación base sólo podría establecerse una comunicación estando fuera de los edificios (obstáculo) y en este caso la cobertura sería outdoor” (puertas afuera).

Si se debe establecer una comunicación desde un área más alejada, aun estando fuera de los edificios (cobertura outdoor’), se deberá utilizar un teléfono de 3 W (transportable); y si se necesitara hacerlo en los limites de la cobertura de la antena, al terminal de 3 W utilizado se le deberá reemplazar la antena por una antena direccional (yagi). Evidentemente, al colocar la antena yagi el terminal pierde su movilidad, pero mejora su capacidad de comunicación.

Tres consideraciones sobre la conexión de una antena yagi:

- Antena bien direccionada (orientada a la estación base más cercana).
- Cable blindado de baja resistencia (para que no exista pérdida de señal).
- Conexión blindada (para que no exista pérdida de señal).

ANTENAS PARA MÓVILES
ANTENA DE GANANCIA HORIZONTAL
ANTENA DE GANANCIA VERTICAL
ANTENA DIRECCIONAL

Existen distintos tipos de antenas en función de su ganancia y circunstancia de uso. Ganancia es la capacidad de una antena de captar una señal electromagnética y convertirla en un impulso eléctrico. En función de esta característica las antenas de los terminales móviles celulares pueden ser:

- Antenas de ganancia vertical: Son las que se utilizan habitualmente para zonas de montaña.
- Antenas de ganancia horizontal: utilizadas para terrenos llanos porque captan señal de antenas mas alejadas horizontalmente.
- Antenas direccionales: tienen la mayor ganancia de un solo lado. Este tipo de antena se utiliza en zonas alejadas de las estaciones base.

CANALES
825.03 CANAL 1 UPLINK
825.06 CANAL 2 UPL1NK
825.09 CANAL 3 UPLINK

CANAL 1 DOWNLINK 870.03

CANAL 2 DOWNLINK 870.06

CANAL 3 DOWNLINK 870.09

Se llama canal a cada incremento de 30 kHz. dentro de la banda de radiofrecuencias asignada, utilizado para la transmisión / recepción de señal. De los canales asignados, cada operadora utiliza una mitad para que las estaciones se comuniquen con los móviles (canales denominados DOWNLINK), y la otra mitad para que los móviles se comuniquen con las estaciones (canales denominados UPLINK)

AMPS - Advanced Mobile Phone Service

NORMA ORIGINAL - Canales uplink

AMPS (Advanced Mobile Phone Service o Servicio de Telefonía Móvil Avanzado) es el estándar de comunicaciones (analógicas) celulares que se utiliza en Argentina.

Esta norma fue desarrollada en EE.UU. por AT&T-Bell a fines de la década del ‘70. El primer sistema con este estándar se instaló en Chicago en 1983. Es utilizado en toda América, en Australia, etc. (a la fecha, en 37 países que totalizan 20 millones de suscriptores). Este sistema utiliza frecuencias (canales) en la banda de los 800 a los 900 MHz. para transmitir en forma analógica. Está previsto para que haya dos operadoras (régimen de competencia), una en cada una de las dos sub-bandas (la A y la B) en que se divide la banda.

Del espectro de radiofrecuencias asignado a las dos operadoras, originalmente se utilizaron desde los 825.03 MHz. a los 844.98 MHz. y de los 870.03 MHz. a los 889.98 MHz., disponiéndose de 666 pares de canales utilizables, divididos en 333 pares para cada operadora, de ellos 313 pares son utilizados para transmisión de voz y sólo 20 para canal de control (por donde se envían las ordenes a los móviles).

E-AMPS Extended Advanced Mobile Phone Service

Actualmente se utiliza una versión extendida de la norma AMPS, la E-AMPS (Extended Advanced Mobile Phone Service o Servicio de Telefonía Móvil Avanzado Extendido). Los 666 pares de canales (frecuencias) utilizables originales (333 para cada operadora) se ampliaron a 832 (416 para cada operadora). Para ello, se asignaron 5 MHz. adicionales, con lo cual la banda comenzó a utilizarse desde los 824.04 MHz. hasta los
893.97 MHz..
La mitad de los canales asignados se utilizan para que el sistema se comunique con los móviles (downlink: 869.04 a 893.97 MHz.) y la otra mitad para que los móviles se comuniquen con el sistema (uplink: 824.04 a 848.97 MHz.).

CLUSTER AMPS

Se denomina cluster (en inglés significa grupo o racimo) a un conjunto de celdas, entre las que una operadora, en un determinado lugar, puede dividir todas sus frecuencias asignadas.
Cuando una operadora reparte sus 416 pares de canales (originalmente, 333) en siete celdas (hasta 57 pares de canales de voz por celda), conforma un cluster de siete celdas. En consecuencia, un grupo determinado de canales usado en una determinada celda del cluster A, puede ser re-usado en una celda del cluster B.

RE-USO DE FRECUENCIAS

Para poder re-usar las frecuencias utilizadas en una cierta celda en otra celda cercana pero no contigua, es necesario usar frecuencias de la magnitud de las que se usan en FM porque ello permite direccionar y acotar el alcance de la emisión.

Cada operadora dispone de 416 pares de frecuencias utilizables en toda su Región de Servicios. Como cada usuario emplea uno de ellos para una comunicación, para aumentar la capacidad de servicio se necesita re-usar dichas frecuencias una y otra vez.

Cuando con las mismas frecuencias se debe dar servicio a más clientes, es necesario que una antena dé servicio a una zona limitada (celda) más pequeña, armar más grupos de esas celdas más pequeñas (que cubran la misma superficie que el cluster original), repitiendo el uso de los 416 pares de frecuencias disponibles. Como se indica, en el cluster B se usan las mismas frecuencias que en el cluster A, de manera que no se utilizan las mismas frecuencias en celdas contiguas. Sin embargo, llega un momento en que esto también resulta insuficiente en áreas de alta densidad de usuarios, ya que existe un límite para la reducción del tamaño de una celda, lo que imposibilita un nuevo re-uso de las frecuencias. Es en ese momento cuando el Gobierno debe licitar nuevas licencias móviles (PCS) en otra banda.

Para el diseño de una red (cobertura en función del tamaño, disposición y cantidad de celdas), hay dos grandes factores que se toman en cuenta: la densidad de usuarios y la topografía de la región (por ejemplo, en regiones montañosas se requieren más antenas que en zonas de llanura).

TIPOS DE CLUSTERS

4 CELDAS
7 CELDAS
12CELDAS
21 CELDAS

Un cluster es un conjunto de celdas adyacentes entre las cuales no se puede efectuar el re-uso de frecuencias. El tamaño de las celdas, su número y la cantidad de canales de cada una debe estar en equilibrio: cuanto menor es el número de celdas, mayor es el número de canales en cada una. En ese caso, la distancia entre celdas que usan los mismos canales es menor y aumenta posibilidad de interferencia entre canales iguales (interferencia co-canal). Dado que la cantidad de celdas depende de la cantidad de usuarios (tráfico de llamadas) y de la topografía del terreno, según los requerimientos de cada área se pueden usar clusters de 4, 7,12 y 21 celdas. En algunas áreas no es necesario instalar más de una celda.

SECTORIZACIÓN DE CELDAS

Dentro del sistema AMPS, es una técnica que permite dividir la celda en sectores, utilizando antenas direccionales. Por ejemplo, con antenas de 120~ de cobertura, que van montadas en la misma torre se la divide en tres sectores.

La sectorización permite una estructura con celdas de menor tamaño, servidas por estaciones base de menor potencia y sin interferencia entre grupos de canales iguales entre celdas más cercanas; de este modo se puede aumentar el número de usuarios con la misma cantidad de frecuencias. Para ello, en una estación base se utiliza una torre para instalar varias antenas direccionales.

La sectorización de celdas es útil en localidades donde no se pueden montar demasiadas torres y se requieren más antenas. En el ejemplo, en lugar de colocar tres torres con antenas omnidireccionales, en una sola torre se montan tres antenas direccionales de 120~ de cobertura cada una.

CANALES - Uso

Voz y Digitales

A los fines de la comunicación celular, las frecuencias de cada sub-banda (A y B) se utilizan en forma de canales, siendo un canal cada incremento de 30 kHz dentro del espectro radioeléctrico. De acuerdo a su uso, hay dos tipos: canales de control o señalización y canales de voz, necesarios para establecer y luego mantener la comunicación, respectivamente.

A su vez, los canales se dividen, según su forma de transmisión, en analógicos y digitales.

CANALES DE CONTROL

Los canales de control son los que transmiten todos los pedidos de iniciación de llamada y de servicio. Hay canales de control en ambos sentidos separados por 45 MHz.: el FCC (‘Forward Control Channel’ - Canal de Control Hacia el Móvil) y el RCC (Reverse Control Channel” - Canal de Control hacia la estación base), a razón de un par de canales analógicos y/o digitales por sector.

Aún cuando los terminales móviles no están en el curso de una llamada activa (en modo de reposo - “stand by’), si están encendidos en el área de cobertura de una antena, están en diálogo constante con el sistema:

Para indicar su ubicación, periódicamente emiten su identificación a través del canal de control; la antena la capta y la transmite al sistema.

A su vez, continuamente monitorean los canales de control de las estaciones base; en primer lugar, para indicarle al usuario cuál es la intensidad de señal del canal de control y, además, para detectar si es que la estación base emitió un mensaje (“paging message”) con la identificación del móvil, pues cuando una llamada tiene como destino un móvil, el sistema lo busca emitiendo el mensaje a través del FCC de la última antena (y de las circundantes, para prever el desplazamiento del móvil) que captó su identificación.

Cuando un móvil debe comunicarse con la estación base para realizar una llamada, la inicia utilizando un RCC donde transmite su propia identificación y el número del teléfono de destino.

ÁREA DE COBERTURA

CANALES DE VOZ

Los canales de voz son los que se utilizan para mantener una comunicación.

Hay canales de voz en ambos sentidos, separados por 45 MHz.: el FVC (Forward Voice Channel" - Canal de Voz Hacia el Móvil) y el RVC (Reverse Voice Channel' - Canal de Voz hacia la estación base). Cada estación base puede disponer de hasta 96 canales de voz. El número exacto de canales de voz usados en cada celda depende del tráfico de llamadas, madurez del sistema, ubicación de las otras estaciones base, tipo de cluster, etc..

Ante un pedido de llamada el sistema asigna un par de canales de voz, el SAI (tono de audio de supervisión) y el VMAC (código de atenuación de voz del móvil). Si todos los canales están ocupados, el sistema prueba un reintento direccionado con una estación base vecina.

La comunicación comienza una vez que está asignado un canal de voz.

Para una conversación se requieren dos canales (uno para transmitir y otro para recibir), por lo tanto en una celda determinada se podrían mantener, como máximo teórico, 96 conversaciones a la vez.

ÁREA DE COBERTURA

CONTROL DE POTENCIA Y CONTINUIDAD DE LA LLAMADA

El SAI es transmitido a través de un FVC y utilizado para iniciar el “handshaking” (intercambio de información de reconocimiento mutuo). El móvil contesta con un tono idéntico por medio de un RVC. La función del SAI es permitir la distinción de un canal de voz deseado frente a usuarios del mismo canal en otras celdas.

La regulación de la potencia es una función del VMAC. El canal de voz posee, entre otras funciones, la del control de potencia. Es decir que, por medio del canal de voz, al sistema le es posible mantener continuamente el control de la comunicación y regular la potencia de emisión del móvil.

Si está cerca de la antena, el sistema le indica al móvil que no requiere una transmisión de máxima potencia, con lo cual el móvil ahorra la energía almacenada en las baterías. La capacidad de control de potencia del sistema es una función clave definida por la norma AMPS.

El canal de voz, además, le permite al sistema saber qué terminal está usando, qué canal, de qué antena y en qué momento. Cuando el móvil se está trasladando del área de cobertura de una antena a otra, por medio de órdenes a través del canal de voz, el sistema tiene la facultad de cambiar automáticamente la antena que le da servicio, sin que se corte la comunicación.

Este texto continuará mes a mes desarrollando diferentes tópicos de la telefonía celular y el sistema en sí.

(...)

[Como montar tu propio servidor Napster]

La proliferación de esta peculiar forma de intercambio de canciones está siendo posible en gran parte gracias a los servidores gratuitos que los propios usuarios montan, de no ser así los actuales servidores oficiales de Napster estarían saturados. Napster utiliza un protocolo propietario, por lo que es desconocido para cualquier desarrollador de software que no pertenezca a Napster. Pero he aquí los que los gurús del código fuente, sniffer en mano, empezaron a ver que información enviaba y esperaba un cliente de Napster, con lo que lograron reconstruir la comunicación cliente servidor en entornos Napster. Una vez habiendo estudiado el protocolo el resto no se hizo esperar.

Al alcance de todos

Actualmente cualquier persona puede montar su propio servidor de Napster, los requisitos no son difíciles de cumplir: una buena conexión a Internet: los servidores Napster reciben muchas solicitudes de búsqueda y tienen que descargar de los clientes el listado de canciones que comparten, una máquina potente: el proceso de búsqueda de canciones se efectúa en el servidor, por la tanto necesita bastantes recursos de CPU y memoria, es recomendable una tarifa plana de conexión para que no os den una clavada (montadlo en la oficina o facultad XD) y cualquier sistema operativo, ya que, gracias al desarrollo en Java de un servidor Napster, será posible montarlo en cualquier SO que soporte Java.

Una vez cumplimentados los requisitos nos centraremos en ver qué programa servidor nos interesa. Los dos más importantes son el OpenNap y el JNerve. La diferencia entre ellos radica en su código fuente. OpenNap está programado en C, con lo que han desarrollado versiones para Linux (alpha, 386, sparc, ppc), BSDI, Solaris, FreeBSD, IRIX, OS/2 y Windows 95/98/NT/2000 mientras que JNerve lo está en java y le permite ser ejecutado en cualquier sistema operativo que lo soporte.

OpenNap para Windows

La versión 0.32 podéis obtenerla de D:\OFFLINE\SOFTWARE\NAPSTER\opennap32.zip. La página web del programa está en http://opennap.sourceforge.net. Si no queremos modificar mucho la configuración del programa es recomendable que lo descomprimamos en el directorio c:\opennap. Lo primero que tendremos que hacer es configurarlo ejecutando setup.exe.
Los datos que nos pedirá son el nick del superusuario (aquí se le llama 'elite'), su clave y su dirección de correo. Una vez hemos introducido estos datos podremos ejecutar el servidor propiamente dicho, que es el fichero opennap.exe con la configuración que trae por defecto. A partir de ahí al servidor se le accede a través del puerto 8888

Instalad el programa, lo tenéis en D:\OFFLINE\SOFTWARE\NAPSTER\setupl38.exe. Una vez hecho esto os apatur de la carpeta del programa Napster. A continuación tendréis que parchear el cliente; para aplicar el parche no debéis estar usando el Napster (aseguraros de que no aparezca su icono en la barra de tareas). Si utilizáis el Napster V2.0 Beta 6 tendréis que utilizar el parche que os damos por separado en D:\offline\software\napster\patch.exe, si no utilizad el que os ha instalado el Napster Server Manager.

Una vez parcheado podemos usar el Server Manager, basta con ejecutarlo (se quedará residente, al igual que hace el Napster) y pulsar "Enter IP". Los datos a introducir son la IP y el puerto del servidor, en nuestro caso será 127.0.0.1:8888.

Ahora podemos utilizar el Napster para conectarnos a nuestro servidor. Para poder trabajar en él tendremos que conectarnos con los datos de superusuario que habíamos especificado al ejecutar el setup.exe.

Como los clientes de Napster no soportan por lo general la administración remota de servidores tendremos que comunicarnos con el nuestro a base de mensajes. Estos mensajes se los dirigimos al pseudousuario OperServ que viene creado por defecto, de esta manera él recibirá los comandos y será quien los ejecute. Sólo admitirá comandos que procedan de usuarios con nivel de moderador o superior. Los niveles de usuario que posee el Napster, ordenador de menor a mayor relevancia, son:

leech, user, moderator, admin y elite. La forma en la que nos comunicamos con OperServ es escribiendo en la línea de mensajes frases siguiendo este formato (donde < >es obligatorio y [ ] es opcional): <comando> <usuario de destino> <mensaje> [opciones]. De esta forma para enviarle un mensaje a OperServ empezaríamos escribiendo "/msg operserv".
Los mensajes que se le pueden enviar a OperServ, reconocidos también por los servidores Napster originales, son: cban, cbanclear, cbanlist, chanlevel, cloak, cunban, config, connect, disconnect, kick, killserver, links, reconfig, register, stats, usermode. OperServ también reconoce otros mensajes que han sido implementados como novedad sólo en el OpenNap. Existe otro pseudo-usuario, el ChanServ, que se encarga de la conf iguración de los canales de chat. Para obtener un listado de sus opciones ejecutad '/msg chanserv help". Si queréis mostrar un mensaje de bienvenida cada vez que un usuario se conecta deberéis crear un fichero llamado "motd" *(message of the day"*, mensaje del día) en el mismo directorio que tengáis el servidor con el texto que queréis mostrar.

Para modificar la configuración del OpenNap tendremos que crear un fichero llamado 'config", al igual que con el "motd". Conviene que utilicéis como base el de ejemplo que trae la distribución: sample.conf. A continuación os detallamos las opciones de configuración que podéis especificar (VER CUADRO). Como veréis, no será por falta de opciones. Hay unas poquitas más, pero son para los linuxeros.

La lástima de esta versión de código libre es que, como no disponen del protocolo completo, no pueden conectar el servidor a servidores Napster oficiales, aunque sí pueden hacerlo entre ellos ☺. La forma de hacer esto es la siguiente:
1.- Creamos otro fichero, en este caso se llamará "servers"
2.- Indicamos en cada línea el servidor a conectar de la siguiente manera: <nombre del servidor> <clave del servidor al que conectar> <clave del servidor propio>
3.- Ahora nos conectamos con nivel de elite a nuestro servidor y mandamos este mensaje: /msg operserv connect <servidor al que conectar> <puerto>
Mediante el uso de la clave del otro servidor y de la propia nos aseguramos que sólo se interconectan servidores cuyos superusuanos están conformes con la unión, así nadie que no queramos chupará información de
nuestros usuarios ☺.

Linux version

La versión 0.34 podéis obtenerla de D:\OFFLINE\SOFTWARE\NAPSTER\opennap-0.34.tar.gz. Sólo debéis descomprimir y compilar el código fuente. Todo funciona de igual manera en todas las plataformas, aunque en Linux es recomendable instalarlo en /usr/local/share/opennap.

Jnerve bajo Windows
Este programa es más sencillo de usar y, a su vez, con menor potencia que el OpenNap ya que llevan poco tiempo desarrollando su código. Su web se encuentra, al igual que el OpenNap, en http://jnerve.sourceforge.net. Para poder utilizarlo en Windows necesitaremos instalar primero el Java Runtime Enviroment, de esta forma podremos ejecutar programas con código fuente escrito en java. Tenéis el JRE en D:\OFFLINE\SOFTWARE\ NAPSTER\jre1_2_2-win-i.exe. Como puede que necesitéis también el Java Development Kit (JDK), os lo hemos puesto en D:\OFFLINE\SOFTWARE\NAPSTER\jdkl2-win32.exe. Una vez instalados podréis descomprimir el JNerve de D:\OFFLINE\SOFTWARE\NAPSTER\jnerve0.32.tar.gz. En el directorio donde lo descomprimáis tan sólo tenéis que ejecutar el fichero startApp.bat para que se arranque vuestro servidor.

Si queréis hacer modificaciones al servidor deberéis editar el fichero jnerve.properties. Os recomendamos que, para no complicarle la vida a vuestros usuarios, pongáis a true la opción de "OpenDoor". Esta opción lo que indica es que aunque un usuario no esté en la lista de usuarios de servidor se le permita el acceso. A este servidor hay que especificarIe la IP de vuestra máquina específicamente en la opción metaserver.server_list.

No os comentaremos el fichero de configuración de este servidor ya que es parecido al del OpenNap y podréis entenderlo sin excesiva dificultad.

JNerve para pingüinos

Idem de lo mismo, os hemos incluido el JRE en D:\OFFLI NE\SOFTWARE\NAPSTER\jre-1.2.2-RC4-linux-i386-glibc-2.1.2.sh y el JDK en D:\OFFLINE\SOFTWARE\NAPSTER\jdk-1.2.2-RC4-linux-i386-glibc-2.1.2.sh (ambos son autodescomprimibles).
El servidor en si es el mismo que para Windows, por lo tanto ya sabéis donde está. Para utilizar este servidor en este SO primero tendréis que ejecutar el makejar.sh para compilarlo, después (calma, que no tarda demasiado) ejecutad el startApp.sh para lanzarlo y empezar a servir MP3. Las instrucciones que acompañan a los programas no son como para tirar cohetes, pero esperamos que os hayáis enterado de lo fundamental.

Como habréis podido comprobar no es demasiado difícil montar tu propio servidor Napster. Podréis sentiros orgullosos de fomentar el libre intercambio de canciones entre usuarios, aunque recordad que también estáis reduciendo las ganancias de esas macrocompañías internacionales y esos cantantes que se duchan con agua mineral y cenan en un país distinto del que desayunaron.

Administración del servidor
Los servidores Napster no traen un programa para trabajar sobre ellos on-line, la única forma de trabajo es utilizando un cliente Napster o un programa específico para ello.

La administración del mismo se realiza a través de clientes de Napster, desde la ventana de mensajes (con comandos similares a los utilizados en el IRC). Para aquellos que utilicen como cliente de Napster el programa oficial habrán observado que no se le puede especificar a qué servidor queréis conectaros. Esto es un problema que solventaremos utilizando el **Napster Server Manager**
v.1.3.8. Este programa nos permite, tras parchear el cliente de Napster, obligarle a conectarse al servidor que nosotros queramos, que en este caso será el nuestro propio.

Un cliente más específico para la administración es el que veréis más adelante, el BWap.

Clientes / Servidores
Las redes Napster no serían nada sin los usuarios, que son quienes realmente tienen los servidores. ¡Son tus usuarios los que distribuyen los MP3! Así que tranqui, de momento los MIG no podrán detenerte por piratería ;-D. Vamos a comentaros algunos gratuitos interesantes.

BWap
Se trata de un programa cliente/servidor de Napster, tiene una apariencia de cliente de IRC en formato texto. Tiene soporte nativo para trabajar en servidores OpenNap, con lo que no es mala idea utilizarlo para trabajar en vuestro servidor OpenNap. No tiene página web, pero sí un FTP que podréis visitar para actualizar vuestro programa: ftp://ftp.bitchx.com/pub/BWap/

En D:\OFFLINE\SOFTWARE\NAPSTER\bwapl4.zip tenéis la última versión del programa para Windows y en la misma ruta con el nombre de bwap-1 .3.tar.gz tenéis la versión para Linux. Vamos a comentaros cómo instalar la versión para Windows ya que los linuxseros soléis ser más “manitas”.

Descomprimid el fichero en C:\BWap. Podéis arrancarlo ejecutando el fichero bwap.exe, aunque os recomendamos utilizar un fichero de proceso por lotes (.bat) para que os arranque directamente con vuestra configuración. Os viene un ejemplo en el fichero sample.bat. Básicamente lo que tenéis que poner en ese fichero es:
set NAPSERVER=nombre_de_vuestro_servidor:puerto:nick:clave:0
set NAPNICK=nick_por_defecto
set NAPPASS=clave_por_defecto
set HOME=//c/BWap **bwap.exe**

A los comandos que queráis ejecutar como superusuarios del servidor deberéis anteponerle /admin. Cuando os hartéis del programa introducid el comando /quit y lo cerraréis.

Napster Libre
Bueno, como no podía ser de otra manera, en Linux también tenemos multitud de programas que nos permiten conectarnos con servidores napster. Los podemos encontrar para todo tipo de entornos, los hay desarrollados en java, los hay desarrollados expresamente para entornos gráficos muy extendidos como pueden ser Gnome y KDE, los hay para las Xwindow en general y los hay para consola. Como veis, los hay de todos los colores y para todos los gustos.

Nosotros vamos a ver en este artículo dos clientes de napster: Knapster 0.12 y Gnome-Napster 0.6.1.

Knapster

Knapster es un programa para KDE equivalente al cliente de Windows del Napster "oficial". Es una versión que todavía se está desarrollando pero que tiene la gran mayoría de características de aquél e incluso alguna más. Entre las pocas cosas que requiere para funcionar, tenemos que destacar que hace falta las KDE y la librería qt 1.44. Para aquellos que hayan instalado ya la versión 2 de **KDE,** decir que se está trabajando en el código para sacar una versión para dicha versión, así que tendréis que esperar un poquito. Para que veáis el aspecto del programa, aquí van algunas fotos de él:
En la pantalla principal, dentro de la pestaña de consola, podéis ver todos los mensajes que indican el estado del programa así como también muestra los mensajes del canal, usuario y los mensajes de error.

En la pestaña de "librería mp3", podéis encontrar los ficheros que compartís. Las canciones pueden ser compartidas o no por directorios. En fin, combinaciones de configuración. Ya que hablamos de configuración, vamos a ver las pantallas correspondientes a dicha configuración. Para empezar, podéis ver la pantalla donde tenéis que meter vuestro login y password si ya tenéis cuenta o, si sois nuevos, activar el cuadro "new user".

Para configurar las diferentes opciones de la conexión, tenéis que ir a la pestaña "connection". Como podréis observar nos viene de peñas la opción de especificarle el servidor y puedo al que queremos conectarnos, de esa forma podremos acceder a nuestro servidor sin necesidad de utilizar programas extra. Otra de las buenas opciones que trae es que podemos modificarle cada vez que queramos el nombre de usuario, así no os ocurrirá como el la versión de Windoze en la que, una vez introducido nuestro nick, no podéis modificarlo mediante el programa. Para configurar las canciones que quereis
tenéis que entrar en la pestaña titulada "Library path". En ella podéis decir qué directorios queréis compartir y cuales no. Ninguna de las opciones del programa es difícil de entender... siempre y cuando estéis acostumbrados a desenvolveros en el idioma guiri.

Como habéis podido ver, este cliente es muy, pero que muy completito y para ponerlo en marcha lo tenéis en O:\OFFLINE\SOFTWARE\NAPSTER\KNAPSTER.

Knapster

Si el anterior cliente/servidor era para KDE, éste lo es para Gnome. En las últimas versiones de ambos gestores se está implementando una especie de interfaz que permite a los usuarios de Gnome usar aplicaciones para KDE y a los de KDE usar aplicaciones de Gnome. Lo único que hace falta es tener las librerías que usan dichos gestores, principalmente, las Qt o GtK.

Este cliente, al igual que el anterior, está todavía en desarrollo y, por ello, no tiene todas las opciones disponibles. Por ejemplo, cabe destacar una muy llamativa que es la ausencia de la posibilidad de subir canciones. Es decir, con Gnome Napster sólo podemos bajar canciones (no creo que eso le importe demasiado a la cantidad de sanguijuelas que hay por ahí XD). A favor Gnome Napster tiene la interfaz gráfica que resulta muy vistosa y útil.

Lo primero que tenemos que hacer es meter nuestro login y password o darnos de alta en el menú que os sale al principio, precisamente, el que podéis ver a continuación:

En dicha imágen podéis observar una opción bastante útil. Dicha opción consiste en permitir que el cliente reintente conectarse automáticamente cada vez que la conexión no es posible por cualquier motivo. Además, también podéis ver como permite la especificación de un servidor en concreto y modificar todos vuestros datos (nick incluido).
Si os dais cuenta, las opciones que nos proporciona este programa son las mismas que las del programa "oficial".

También, como no podía ser de otra manera, tiene la parte dedicada a la configuración o preferencias. Como buen programa Linux nos permite más opciones que las versiones para Window$, cosa que nos será muy práctica a la hora de conectar a nuestro servidor.

Como decía ese gran gurú" Querido discípulo, practica, practica". Los seguidores de Gnome que queráis seguir sus enseñanzas debéis poner rumbo a D:\OFFLINE\SOFT-

WARE\NAPSTER\GNOME NAPSTER.

En definitiva, ambos clientes son bastantes buenos aunque les quedan cosas por pulir y otras por desarrollar pero seguro que cuando estén completamente terminado son dos de los grandes.

{fin adjunto el cuadro de comandos}

Cuadro de Comandos

Parámetro	***Explicación***
server_name	Para indicar el nombre del servidor (necesitaréis un nombre reconocido por las DNS)
server_password	La clave para interconectar otro servidor con el nuestro
server_ports	Puertos en los que espera conexión el servidor. Se le pueden especificar varios
max_user_channels	Número máximo de canales en los que puede estar un usuario, se utiliza para que no consume demasiado ancho de banda ese usuario
max_nick_length	Número máximo de caracteres que puede tener un nick. Cuidadín con poner una cantidad muy grande porque algunos clientes Napster pueden hacer cosas raras si un usuario tiene como nick ‘supercalifragilisticoespialídoso”
Server_queue_length	Número máximo de elementos en la cola de interconexión entre servidores. Si veis que vuestro servidor empieza a renquear o a cargarse demasiado reducid este valor porque las múltiples búsquedas de los usuarios os pueden ahogar la máquina
client_queue_length	Idem que el anterior, pero en esta ocasión es para evitar que un usuario nos sature
max_browse_result	Número máximo de elementos que puede mostrar una solicitud de exploración
max_resulta	Número máximo de canciones que puede mostrar una solicitud de búsqueda
max_shared	Número máximo de canciones que puede intercambiar un usuario. Dejad este valor como está y, si hay algún usuario que tenga un mayor número de canciones id probando a subirlo
stat_click	Cada cuantos segundos enviarle un mensaje de estado del servidor a los clientes. Poned un valor alto (unos 60 segundos) para no consumir mucho ancho de banda
max_connections	Número máximo de conexiones. Si queréis ser “importantes” ampliad el valor o habrá tan pocos clientes en vuestro servidor que poca gente querrá conectarse a él (o ponedle un valor bajo e interconectaros con otros
collect_interval	Segundos entre ejecución de la colección de basura
listen_addr	IP en la que está vuestro servidor
config_dir	Directorio en el que se almacenan los ficheros de configuración. Si lo dejáis con .‘ será el directorio actual del programa
channel_limit	Máximo número de usuarios en un canal. Puede ser un valor alto ya que pocos usuarios se conectan a los canales (suele ir a saco a buscar canciones (¿para qué hablar con nadie?)
login_timeout	Máximo número de segundos que puede estar un usuario inactivo, después de ese tiempo es desconectado

max_command_length	Número máximo de caracteres que puede contener un comando,
en	tendréis que tener cuidado de no poner un valor corto porque ese comando van los nicks, nombres de canales.., y suman muchos caracteres
auto_register hacer rechazado	Si un usuario no está registrado en vuestro servidor podréis que se registre automáticamente (valor 1") o que sea hasta que obtenga un nombre de usuario aceptado "0'
registered_only	Sólo permite conectarse a vuestro a usuarios registrados, cosa que no mola a no ser que montéis una red privada
max_hotlist	Número máximo de entradas que puede tener una hotlist
max_ignore ignorar	Número máximo de entradas que puede tener una lista de
max_topic	Tamaño máximo que puede tener el tópico de un canal
max_client_string de	Número maximo de caracteres que puede contener la version un cliente (una chorrada de opción)
max_reason de	Número máximo de caracteres que puede contener el motivo un kill, baneo... (se pasan con tantas opciones, coñe
max_path de	Número máximo de caracteres que puede contener el nombre los ficheros
compression_level	Nivel de compresión

Cabe destacar que el autor de este artículo es Andrés Méndez y el mismo salió publicado en la Revista @rroba #35

Los files nombrados en este artículo puedes encontrarlos en nuestra web page.

Reproducido y elaborado por (...)

Hackeaste algo? Decinos Qué, Cuando y Cómo !!!

Esta sección es en donde vos podrás expresarte y contarnos si es que alguna vez hackeastes una page o server como lo haz hecho, debidamente documentada. Con esto que queremos decir... que no venga alguien y nos diga, “yo lancé un misil de la NASA! pero no tengo una pantalla capturada ni un documento que lo sostenga”, eso no va. Si querés compartir info con nosotros este es tu lugar. Para participar de esta sección, envíanos un mail a Maritxa1998@hotpop.com

Chau hasta la mHz # 2 !!!